TITLE OF THE INVENTION

AUTHENTICATION FOR USE OF HIGH SPEED NETWORK RESOURCES

INVENTORS
Philip Cunetto
James M. Doherty
Chien-Chun Lu
Timothy Schroeder

P19740.S04

AUTHENTICATION FOR USE OF HIGH SPEED NETWORK RESOURCES

BACKGROUND OF THE INVENTION

1. Field of the Invention

[0001] The present invention relates to the field of telecommunications. More particularly, the present invention relates to associating a request for a switched virtual circuit (SVC) service in a high speed network to an originating subscriber, so that the network can apply the subscriber's individual service policies, and optionally registering an access port address to the subscriber.

2. Background Information

[0002] Currently, when network subscribers access a high speed network for SVC services, the port being used for the access is associated with the SVC service request. Thus, if multiple subscribers could access the network from a single port, each subscriber would not be uniquely associated with the network access. Similarly, if a subscriber could access the network from a location remote from the subscriber's normal access port (e.g., accessing from a public access port), the subscriber is not associated with the network access. In both cases, because the port is associated with the network access rather than the subscriber, control of access to the network is inadequate.

[0003] In a conventional telephone network, access requests do not require control for several reasons. For example, each connection across the network consumes a predetermined amount of bandwidth, regardless of the application employing the connection. In addition, a user in a conventional telephone network is limited to a single connection at each physical interface. In other words, there are natural, systematic limits on the resources a single subscriber is able to consume in the telephone network.

[0004] In high speed networks, a single connection can consume the bandwidth of many thousands of conventional telephone network connections. Moreover, many connections can be simultaneously active on a single interface to the network. Thus, due to the potential for depletion of available resources, authorization on a per connection request basis is more important in a high speed network than in the conventional public switched telephone network (PSTN). Accordingly, there is a need for reliable authentication and control of subscriber access to high speed networks.

[0005] High speed networks, such as ATM networks, are often configured to use switched virtual circuits (SVCs), which are temporary connections established by the user at the time of call set-up. SVCs generally provide a flexible bandwidth adjusted to accommodate the application being supported by the connection. Typically, customers using SVCs pay a network provider on a per connection time basis, as opposed to paying monthly fees, as for permanent connections. In high speed networks, the bandwidth and SVCs themselves are both limited network resources. Therefore, from the network provider's point of view, each request from a subscriber to establish an SVC must be policy checked to determine if the subscriber has the right to the requested resources, as based on a prior service level agreement.

[0006] Furthermore, high speed network subscribers are often groups of users as opposed to individual users. Each group is allocated a combined set of resources, including SVCs and bandwidth, collectively available to the entire group at any one time. Again, close monitoring of the use of group allocated resources is necessary to avoid overcrowding and interference on the network and consumption in excess of the services contracted for by the users.

[0007] When a subscriber requests access from a network assigned, non-shared location, the network can identify the port requesting access and can identify the

subscriber based upon a known association between the fixed port and the subscriber. In the case of nomadic users, however, ports are not associated with subscribers, preventing simple identification of nomadic users. Thus, remote port SVC connections do not provide the subscribers with the service policies to which the subscribers are entitled.

[0008] Furthermore, even when a subscriber originates a request from a fixed port, existing methods are able to associate only one user at a time with the fixed access port. This restriction is problematic when multiple subscribers require access to a single port, and when a single subscriber has multiple subscriber identities from the network's point of view, e.g., each identity has a different service policy.

[0009] Establishing a connection to a virtual private network, such as an ATM network, is well known in the field of telecommunications. For example, TELLO et al., U.S. Patent No. 6,032,118, teach a method for accessing (and billing) a virtual private network through a data network from a remote location using terminals, such as desktop, laptop and notebook computers. The method of TELLO et al., however, is limited in that the authentication steps are cumbersome and inconvenient. In particular, the user must affirmatively select the identification and password and a virtual private network. An encryption key is then sent to the user, along with an authorization code upon password verification. Also, the method of TELLO et al. does not provide a registration process, by which the virtual private network would "memorize" the user's remote location and treat it as part of the network. Therefore, the user must repeat the authentication process each time access is attempted, even if using the same port.

[0010] The overarching need is to enable subscribers to a high speed network to access that network, even when calling from a remote location, so that appropriate corresponding service policies may be implemented. Also, the need includes

permitting a nomadic subscriber to associate the temporary physical address with the subscriber's network for as long as the subscriber desires. Currently, the high speed networks and associated SVC connection systems do not meet these needs.

BRIEF DESCRIPTION OF THE DRAWINGS

[0011] The present invention is further described in the detailed description that follows, by reference to the noted plurality of drawings by way of non-limiting examples of embodiments of the present invention, in which like reference numerals represent similar parts throughout several views of the drawings, and in which:

[0012] Fig. 1 is a block diagram showing an exemplary telecommunications network, according to an aspect of the present invention;

[0013] Fig. 2 is a block diagram showing an exemplary telecommunications network involving a nomadic user, according to an aspect of the present invention;

[0014] Fig. 3 is a flowchart showing an exemplary process for registering an access port with an ATM network, according to an aspect of the present invention;

[0015] Fig. 4 is a flowchart showing an exemplary process for de-registering an access port from an ATM network, according to an aspect of the present invention;

[0016] Fig. 5 is a flowchart showing an exemplary process for automatically authenticating a subscriber requesting a switched virtual circuit (SVC) connection to an ATM network and automatically registering the access port, according to an aspect of the present invention;

[0017] Fig. 6 is a flowchart showing an exemplary process for automatically authenticating a subscriber requesting an SVC connection to an ATM network and interactively registering the access port, according to an aspect of the present invention; and

[0018] Fig. 7 is a flowchart showing an exemplary process for interactively authenticating a subscriber requesting an SVC connection to an ATM network and interactively registering the access port, according to an aspect of the present invention.

DETAILED DESCRIPTION OF EMBODIMENTS

[0019] In view of the above, the present invention through one or more of its various aspects and/or embodiments is presented to accomplish one or more objectives and advantages, such as those noted below. It is noted that although the embodiments described below are described with reference to ATM networks, any high speed network employing SVCs, such as an IP network and an optical network, can operate according to the principles of the present invention.

[0020] An aspect of the present invention provides a method for associating a switched virtual circuit (SVC) connection request in a high speed data network with a network subscriber. The method includes receiving a signaling protocol message requesting the SVC connection from the subscriber at an access port and determining whether the signaling protocol message contains authentication data to authenticate the subscriber. The access port may be different from a permanent access port of the subscriber. When the subscriber is authenticated, the SVC connection request is assoicated with data from an account corresponding to the subscriber. The method may further include retrieving service policies from the subscriber account; determining from the service policies whether the subscriber is entitled to access the network from the access port, as requested; and enabling access to the high speed network when the service policies entitle the subscriber to make the requested access. An address of the access port in the network may be registered by substituting the address of the access port for an existing subscriber address.

[0021] Another aspect of the present invention provides a method for associating an SVC connection request from one of multiple subscribers at a single access port in a high speed data network, which includes receiving a signaling protocol message requesting the SVC connection from the access port. The signaling protocol message includes multiple data fields. Authentication data is retrieved from at least one of the data fields and compared with multiple network subscriber accounts. The SVC connection request is associated with the network subscriber account corresponding to the authentication data. At least one other of the subscribers can request simultaneously an SVC connection from the same access port.

[0022] A network access port address corresponding to the access port may be retrieved from a second one of the data fields. A registration address associated with the network subscriber account may then be changed from an original access port address to the network access port address. Furthermore, at least one connection request may be received from another user of the high speed network, where the request is directed to the subscriber. The connection request is terminated to the registration address.

[0023] Another aspect of the present invention provides a method for associating a network policy with a subscriber in an ATM network, which includes rights for establishing an SVC connection. The method includes interfacing between the ATM network and the subscriber through an ATM compatible access port; receiving at the ATM network a conventional signaling protocol message requesting the SVC connection; and determining whether the signaling protocol message contains a first identification number associated with the subscriber. When the signaling protocol message contains the first identification number, it is determined whether the signaling protocol message contains a second identification number that correctly corresponds to the first identification number. The first identification number may

include a publicly known number associated with the subscriber and the second identification number may include an encrypted private password associated with the first identification number. When the signaling protocol message contains the correctly corresponding second identification number, the service policy is retrieved from an account associated with the first identification number and the second identification number. It is determined whether the retrieved service policy permits the subscriber to establish the SVC connection. The SVC connection is established when permitted by the retrieved service policy. The signaling protocol message may include a SETUP message, in which the first identification number may be contained in a first predetermined field and the second identification number may be contained in a second predetermined field.

[0024] The method may further include registering an address of the ATM compatible access port. The registration includes retrieving the ATM compatible access port address from a signaling protocol message, retrieving from a registration database registration data associated with the subscriber and replacing the predetermined ATM address with the ATM compatible access port address retrieved from the signaling protocol message. The registration data includes a predetermined ATM address.

[0025] Another aspect of the present invention provides a method for registering an access port of a subscriber in a high speed data network and includes establishing a connection between a subscriber terminal and a network registration database from the access port, retrieving from the registration database a registration address associated with the subscriber and replacing the registration address with an address of the access port. Connection requests directed to the subscriber are terminated at the address of the access port, indicated as the registration address associated with the subscriber. Also, prior to retrieving the registration address associated with the

subscriber, the subscriber is authenticated. When the subscriber is successfully authenticated, the service policies corresponding to the subscriber are retrieved.

[0026] The address of the access port may be different from an address of a preexisting access port of the subscriber. The method then includes replacing the registration address with the address of the preexisting access port prior to the subscriber disconnecting from the high speed network. Connection requests directed to the subscriber are terminated at the address of the preexisting access port, indicated as the registration address associated with the subscriber.

[0027] Another aspect of the present invention provides a system for processing an SVC connection request in a high speed data network, including a registration server that stores at least one identification number associated with a network subscriber, a database that stores at least one policy defining permission to establish SVC connections and at least one switch in the high speed data network that accesses the registration server and the database. The switch is accessible by at least one access port, connectable to the switch, which enables the network subscriber to interface with the high speed data network from a subscriber terminal. The switch receives a protocol message from the subscriber terminal requesting the SVC connection from the access port, accesses the registration server to determine whether the protocol message contains valid authentication data, retrieves the at least one policy associated with the network subscriber from the registration database when the protocol message contains valid authentication data, and establishes the SVC connection according to the at least one policy. The access port may be different from a previously established access port of the network subscriber. Also, the server may register an address of the access port in place of an address of the previously established access port associated with the ATM subscriber.

[0028] An aspect of the present invention provides a system for processing services of a subscriber in an ATM network, including establishing an SVC connection. The system includes a registration server that stores authentication data associated with the subscriber; a service database that stores at least one ATM policy for establishing the SVC connection; and at least one ATM switch that accesses the registration server and the service database. The authentication data includes an identification number and a password. The ATM switch is connectable to an access port that enables the subscriber to interface with the ATM network from a subscriber terminal. The registration server determines whether a signaling protocol message requesting the SVC connection, received from the access port, includes the identification number and the password associated with the subscriber. When the protocol message includes the identification number and the password, the ATM switch accesses the service database to determine the ATM service policies associated with the subscriber and processes the SVC connection request according to the ATM service policies.

[0029] The authentication data may be contained in at least one of multiple pre-determined fields of an ATM SETUP message of the signaling protocol message. The registration server may store an address of the access port contained in one of the predetermined fields and substitute the stored address of the access port for a preexisting address of another access port of the subscriber.

[0030] Yet another aspect of the present invention provides a system for registering an access port of a subscriber in an ATM network, including a registration server that stores an original port address as a registration address associated with a subscriber and at least one ATM switch in the ATM network that accesses the registration server. The ATM switch is connectable to at least one access port that enables the ATM subscriber to interface with the ATM network from a terminal. The ATM switch interfaces the terminal to the registration server from the access port. The

registration server changes the registration address from the original port address to an address corresponding to the access port, such that subsequent ATM network connection requests directed to the subscriber are terminated at the terminal via the access port. The registration server may store the address of the access port in place of the original port address when the ATM subscriber instructs the registration server to register the access port.

[0031] Another aspect of the present invention provides a computer readable medium for storing a computer program that associates an SVC connection request in a high speed data network with a network subscriber. The computer readable medium includes a receiving source code segment that receives a signaling protocol message requesting the SVC connection from the subscriber at an access port; an authentication source code segment that determines whether the signaling protocol message contains authentication data to authenticate the subscriber; and an associating source code segment that associates the SVC connection request with data from an account corresponding to the subscriber when the subscriber is authenticated. The computer readable medium may further include a retrieving source code segment that retrieves service policies from the subscriber account; a determining source code segment that determines from the service policies whether the subscriber is entitled to access the network from the access port, as requested; and an enabling source code segment that enables access to the high speed network when the service policies entitle the subscriber to make the requested access. The access port may be different from a permanent access port of the subscriber. There may also be a registering source code segment that registers an address of the access port in the network by substituting the address of the access port for an existing subscriber address.

[0032] Another aspect of the present invention provides a computer readable medium for storing a computer program that registers an access port of a subscriber

in a high speed data network. The computer readable medium includes a connecting source code segment, a retrieving source code segment and a replacing source code segment. The connectiong source code segment establishes a connection between a subscriber terminal, which accessess the high speed data network from the access port, and a network registration database. The retrieving source code segment retrieves from the registration database a registration address associated with the subscriber. The replacing source code segment replaces the registration address with an address of the access port. The address of the access port may be different from an address of a preexisting access port of the subscriber.

[0033] The computer readable medium for storing a computer program may also include a terminating source code segment that terminates connection requests directed to the subscriber at the address of the network access port, indicated as the registration address associated with the subscriber. There may also be included an authenticating source code segment and a servcie policy source code segment. The authenticating source code segment authenticates the subscriber prior to the retrieving source code segment retrieving the registration address associated with the subscriber. The service policy source code segment retrieves a service policy corresponding to the subscriber when the subscriber is successfully authenticated in accordance with the authenticating source code segment. The computer readable medium may further include a replacing source code segment and a terminating source code segment. The replacing source code segment replaces the registration address with the address of the preexisting access port prior to the subscriber disconnecting from the high speed network. The terminating source code segment terminates connection requests directed to the subscriber at the address of the preexisting access port, indicated as the registration address associated with the subscriber.

[0034] The present invention enables a high speed network, such as an ATM network, an optical network, or the like, to dynamically apply the individual service policies of a network subscriber through any compatible interface, or port. Thus, the appropriate service policy can even be applied when the subscriber accesses the network from a port remote from the subscriber's permanent port. Generally, regardless of the port used to access a high speed network, the subscriber will be able to implement the personalized service rights and restrictions applicable to the subscriber. Furthermore, an aspect of the invention enables the network to register an access location of the subscriber for purposes of terminating connections intended for the subscriber to that location, regardless of the port being used for network access. In addition to the obvious convenience to the subscribers, the invention protects the network from unauthorized use of network services and SVC connections, including unauthorized use of excessive bandwidth.

[0034] Fig. 1 depicts a simple exemplary network according to one embodiment of the invention. The core of the system is an ATM network 102. The ATM network 102 is based around a set of ATM capable switches, such as ATM switch 103. Although a single ATM switch 103 is shown, the ATM network 102 can (and usually does) include multiple ATM switches 103. The ATM switches may include, for example, CBX 500 Multiservice Wide-Area Network (WAN) and GX 550 Multiservice WAN switches manufactured by Lucent Technologies, Inc., or Alcatel 7440 Multiservice Switching Platforms manufactured by Alcatel, and associated software. The switches are able to support ATM User-Network Interface (UNI) Specification Version 3.1, or higher, software. The ATM switches of an ATM network are interconnected by point-to-point ATM links or interfaces.

[0035] Also included in the ATM network 102 are a subscriber profile database 110 and a registration server 112. In alternative embodiments of the invention, the

subscriber profile database 110 and the registration server 112 may be incorporated in the switch 103, or the switch 103 may include a duplicate database having the same information as subscriber profile database 110 and the registration server 112.

[0036] The registration server 112 contains the subscribers' respective authentication information, including addresses, identification numbers and/or passwords for accessing the ATM network 102. The subscriber profile database 110 stores the service policies for each subscriber at a memory address corresponding to the subscriber. The service policies define the scope of ATM resources and services available to each subscriber, based on a previously established service agreement between the subscriber and the network operator. The service policies include information about a subscriber's priority, whether a subscriber is entitled to establish SVC connections and, if so, the maximum bandwidth available for the SVC connections. The service policies also include information about the various services to which the subscriber subscribes, including services internal to the ATM network 102 and otherwise accessible through the ATM network 102, such as access to the Internet 120 through an Internet service provider.

[0037] Interfacing with the ATM network 102 is a permanent subscriber location 108. In an embodiment of the invention, the subscriber location 108 is the permanent address with which the ATM network 102 associates the subscriber's ATM network-address and other identifying data, along with corresponding subscriber service policies. Subscriber location 108 may represent a single user or a group of users in a separate network, e.g., a private network (not pictured).

[0038] There are two fundamental types of circuits within an ATM network: permanent virtual circuits (PVCs) and switched virtual circuits (SVCs). The PVC connections are preprogrammed to exist between selected source and destination locations in the network. The SVC connections are temporarily and automatically

established in response to signaling, on a per connection basis. SVCs are more flexible than PVC connections, and therefore may enhance the functionality of routine ATM network operations. The permanent subscriber location 108 may be connected to the ATM network 102 by a PVC connection or an SVC connection, depending on the requirements of the location and the function of the ATM network 102 with respect to the location.

[0039] Fig. 2 is the same as Fig. 1, except that it also depicts a nomadic user terminal 104 connected to the ATM network through a remote ATM access port 106. A nomadic user is a subscriber who is attempting to access ATM network services from a location other than the subscriber's permanent location 108. The nomadic user terminal 104 may be any end terminal capable of accessing the ATM network 102, including, for example, laptop computers, personal computers, notebook computers, mobile telephones, personal digital assistants (PDA) and the like. The nomadic user terminal 104 runs various types of application software 124, which include applications for initiating the SVC connection with the ATM network 102. The application software 124 may include a unique publicly known identification number and associated secure password of the subscriber so that the ATM network 102 is able to recognize the subscriber, as described below.

[0040] Fig. 3 is a flowchart depicting an embodiment of the invention in which the subscriber accesses the network and "registers" the address of the access port to enable termination of SVC connections to the registered address. The registration process associates the subscriber with a particular access port or service. Although the discussion regarding the flowchart of Fig. 3 assumes a roaming subscriber, i.e., a nomadic user, it also relates generally to an alternative embodiment of the invention, in which the subscriber desires to register the address of his or her permanent location 108. Ordinarily, though, the address of the permanent location 108 is set in the

registration server 112 as the "default" registration associated with the subscriber. Once the subscriber registers the address of an access port, the ATM network 102 remembers the registered location and sends incoming SVC connection requests to the registered access port.

[0041] At step s300, the subscriber accesses the ATM network 102 from the nomadic user terminal 104 via the remote access port 106, which in this exemplary embodiment is an access port other than the one with which the ATM network 102 ordinarily associates the subscriber. The remote access port 106 may be any public or private network port capable of connecting with the subscriber's ATM network 102, either directly or through other networks accessible to the subscriber's ATM network 102.

[0042] Accessing the ATM network 102 requires running registration application software 124 at step s302 of Fig. 3. In an embodiment of the invention, the software application 124 asks the subscriber for authentication data, such as a user identification number and password, which the subscriber provides to enable the application software 124. The application software then sets up an SVC to a predefined terminating address of the registration server 112 at step s304. The registration server 112 prompts the subscriber at step s306 for ATM network authentication data, which is stored in the registration server 112. The authentication data may include, for example, an account number and a password, which may be the same as the account number and password entered by the subscriber to activate the application software 124 at step s302.

[0043] Ordinarily, an access port is configured to accommodate only one subscriber at a time for registration purposes because the ATM network 102 associates the registration request with an address of the physical access port. However, the application software 124 can be modified, in conjunction with the ATM

switch 103, to provide access port address information and subscriber identification information embedded in separate fields of a conventional signaling protocol message, as described below with respect to Figs. 5 and 6. The ATM switch 103, along with any intervening ATM switches, would simply need to be configured to propagate the embedded information to the registration server 112. Multiple users would then be able to access the network for registration purposes from a single physical port.

[0044] At step s308, the registration server 112 determines whether the authentication data entered by the subscriber from the nomadic user terminal 104 corresponds to the stored authentication data. When the entered authentication data does not correspond, the registration attempt is terminated. When the entered authentication data does correspond, the subscriber sends a registration command via the application software 124, automatically or interactively, and the registration server 112 sets the registered address associated with the subscriber to match the address of the remote access port 106 at step 310. Thus, the SVC terminating address of the subscriber, previously associated for example with the permanent subscriber location 108, is set to the address of the remote access port 106. The ATM network 102 then correlates the subscriber's personal ATM address with the location address of the network port on which the connection was established, i.e., the remote access port 106. The subscriber may then interact with the ATM network 102 or simply log-off after registering the new address. All future SVC requests from other users addressed to the subscriber's personal ATM address will be automatically routed and terminated at the nomadic user terminal 104 through the remote access port 106.

[0045] Fig. 4 depicts the process by which the subscriber de-registers an ATM access port address. The process is similar to the registration process described with respect to Fig. 3 above. Initially, the subscriber accesses the ATM network 102 at

step 400 from, for example, the nomadic user terminal 104 via the remote access port 106. At step s402, the nomadic user terminal 104 runs the application software 124, which establishes a connection with the terminating address of the registration server 112 at step s404. At step s406 the registration server 112 prompts the subscriber for authentication to access the ATM network. When the registration server 112 determines at step s408 that the authentication is not successful, the de-registration attempt is terminated and the registered address remains the same. When the authentication is successful, the subscriber sends a de-registration command via the application software 124, automatically or interactively, and the registration server 112 sets the registered address to the subscriber's default port address at step s410. The default port address is ordinarily the permanent subscriber location address 108, although an alternative port address may be programmed into the registration server, either by the service provider at the time the account is set up, or interactively at a later time by the subscriber, accessing the registration server 112 via the Internet, for example. The SVC terminating address is again set to the address of the permanent subscriber location 108.

[0046] In an embodiment of the invention, the de-registration process is initiated automatically whenever a session ends and the registered address in the registration server 112 is different from the default port address. When the subscriber indicates a desire to end the session and exit the ATM network by terminating all remaining SVC connections, the registration server compares the registered port address with the default port address. If the two port addresses match, the subscriber is disconnected from the ATM network 102 and the registration address remains unchanged in the registration server 112. If, however, the two port addresses do not match, the registered port address is set to the default port address. In one embodiment, when the two port addresses do not match, the subscriber is notified

prior to logging-off that the registered port address is different from the default port address and queried whether de-registration is desired. If the subscriber indicates a desire to de-register, the terminating address at the registration server 112 is set to the default port address and the subscriber is disconnected from the ATM network 102. Otherwise, the registered port address remains unchanged in the registration server 112.

[0047] Fig. 5 is a flowchart depicting the process of a subscriber accessing the ATM network 102 through remote access port 106 and, in particular, being automatically authenticated for an SVC connection, as well as automatically registered at the current access port. Automatic registration is enabled by setting an auto-register switch associated with the subscriber in the registration server 112 to YES. The auto-register switch is previously set, for example, by the ATM network provider according to the subscriber's service policies, or by the subscriber by connecting to an ATM network provider web page and interactively setting the registration status. The web page may be accessed via an SVC connection in the ATM network or over the Internet, using any Internet compatible device.

[0048] Although Fig. 5 depicts a nomadic user, i.e., a subscriber accessing the ATM network from a port other than his or her permanent subscriber location 108, the authentication process is essentially identical regardless of the subscriber's location and access port. For example, Fig. 5 also depicts generally an embodiment of the invention in which the permanent subscriber location 108 routinely interfaces with the ATM network 102 via an SVC connection established on a per connection basis. Because the subscriber is able to originate the SVC connection request from any access port, though, it is necessary to securely identify the subscriber requesting the connection, so that appropriate personalized service policies are applied.

[0049] At step s500, the subscriber accesses the ATM network 102 from a port other than the permanent access port 108, with which the ATM network 102 ordinarily associates the subscriber. The remote access port may be any public or private network port capable of connecting with the ATM network 102, either directly or through other networks accessible to the ATM network 102. Accessing the ATM network 102 requires running SVC connection software application 124 at step s502. The software application 124 initiates the process by sending a signaling protocol message to request the SVC connection. In the system depicted in Fig. 5, the signaling protocol message is received by the exemplary ATM switch 103 at step s504.

[0050] Authorization of the subscriber is performed by the registration server 112, which receives the signaling protocol message from the ATM switch 103. The signaling protocol message enables authorization and includes, for example, a publicly known user identification number and encrypted password uniquely associated with the user identification number. Significantly, known signaling protocols can be utilized in the signaling protocol message. For example, the subscriber's user identification number can be encoded as an ATM address and stored in the CallingPartyNumber field of an ATM SETUP message sent from the roaming subscriber terminal 104. The encrypted password (e.g., an arbitrary 20 bytes of data) can be similarly stored in the CallingPartySubaddress field of the ATM SETUP message. Any other appropriate sized and available fields within a signaling protocol message may be used for storing user identification numbers and passwords in alternative embodiments of the invention. Furthermore, the conventional signaling protocol message may also include an access port address stored in a third field, which would enable multiple users to register a network address from a single access port (e.g., remote access port 106).

[0051] At step s506, the SETUP message data, which has been forwarded by the ATM switch 103 to the registration server 112, is read for authentication of the subscriber. The registration server 112 first determines at step s508 whether the SETUP message contains a user identification number and, if so, whether the user identification number corresponds to a network subscriber. For example, if the CallingParty-Number is a blank field, or if it contains a number that does not match a current subscriber's user identification number (as indicated in the subscriber data stored at the registration server 112), the registration server 112 instructs the ATM switch 103 to reject the SVC connection request at step s516, terminating the connection process.

[0052] If there is a valid user identification number, the registration server 112 determines at step s510 whether the SETUP message contains an encrypted password and, if so, whether the password corresponds to the user identification number. For example, if the CallingPartySubaddress is a blank field, or if the password contained in the CallingPartySubaddress does not correspond to the user identification number, the registration server 112 instructs the ATM switch 103 to reject the SVC connection at step s516. Again, the registration server 112 contains the preestablished password information associated with the user identification number.

[0053] The SETUP message, including the encrypted password, traverses only a small portion of the subscriber's carrier network, thereby reducing the likelihood of a third party successfully "eavesdropping" to obtain an encrypted password. To further enhance security, the encrypted password is not propagated in subsequent SETUP messages by intervening ATM switches in the connection path, as are most other protocol elements. Instead, the password is removed when used for authentication purposes. The user identification number (e.g., the subscriber's personal ATM address), however, would likely be serving the dual role of

CallingPartyNumber, depending on the specific implementation, in addition to ATM network authentication. The personal identification number is therefore propagated according to current signaling specifications.

[0054] When the user identification and password provided in the ATM SETUP message match, the address of the remote access port 106 is automatically registered in the registration server 112 at step s511 because the registration flag has been set to YES. That is, the existing registered address is replaced by the address of the remote access port 106, as previously described for example with respect to Fig. 3. The automatic registration is transparent to the subscriber, assuring that the most current access port is registered, and thereby enabling the benefits of registration without the subscriber having to take the time to respond to registration related queries. Because there may be times when the subscriber prefers not to remain registered at an access port beyond the current session, the subscriber may invoke the deregistration procedure of Fig. 4 to de-register.

[0055] The personalized service policies associated with the identified subscriber are then retrieved from the subscriber profile database 110 at step s512 by the registration server 112, or alternatively, the ATM switch 103. The personalized service policies are preestablished contractually between the subscriber (or the subscriber's group) and the ATM network provider. Based upon the retrieved service policies, the registration server 112 (or ATM switch 103) first determines at step s514 whether the particular subscriber is authorized to establish SVC connections of the type and bandwidth requested based on the retrieved service policies. If not, the subscriber profile database 110 instructs the ATM switch 103 to reject the SVC connection request at s516, ending the process. If the service policies indicate that the subscriber is entitled to establish the requested SVC connection, the SVC

connection is established from the remote ATM access port 106 to the destination port at step s518. The subscriber may then use the connection.

[0056] Significantly, in an embodiment of the invention, the authentication related steps s504 through s514 are performed transparently to the subscriber. Because the user identification number and password have been previously embedded in the protocol message, there are no interactive steps performed by the subscriber during the connection process. In other words, the ATM network 102 does not query the subscriber to enter any numbers or other information in order to establish the requested SVC connection or to implement the personalized services.

[0057] As a result, the connection process from the remote access port 106 is quick and efficient. Also, the subscriber does not need to memorize numbers or passwords for simply connecting with the network. This is especially advantageous where the subscriber is required to input additional identification numbers and/or passwords to execute selected services within the ATM network 102 after establishing the SVC connection, or to execute selected services connectable through the ATM network 102, such as the Internet 120. Also, the SVC connection request process may be embedded in any ATM related service or application, such as a game program, and is automatically performed each time the subscriber initiates the service or application. Furthermore, the authentication is provided in the same manner regardless of whether the executed service control and policy application is applied directly on the ATM switch or in an off-board connection control processor. It is noted that, in alternative embodiments, the application software 124 includes interactive steps for the subscriber to enter identification number and password information, as discussed below.

[0058] Because the identification and authentication are performed on a per connection basis, multiple users can simultaneously use the same network connection.

The ATM network 102 can accurately associate SVC connection requests to the respective originating subscribers and apply the correct corresponding service policies based on the identification of each subscriber, as opposed to the physical port from which a communication is initiated. Also, a single individual may have more than one subscriber identity from the ATM network's point of view, e.g., a subscriber may pay for a publicly available version of a service, as well as belong to a corporate closed user group with access to the same service with different rights and privileges. In this situation, the individual subscriber has two different user identification numbers, yet is able to receive the correct services for each user identification number on the same access port and simultaneously, if so desired.

[0059] In another embodiment of the invention, an example of which is shown in Fig. 6, registration of the access port is not performed automatically when the subscriber accesses the ATM network to request an SVC connection, per the subscriber's service policies. In particular, the subscriber's auto-register switch is set to NO. The subscriber is therefore provided an option to interactively register the access port in the course of the connection process. Although Fig. 6 depicts a subscriber accessing the ATM network from a port other than his or her permanent subscriber location 108, the process is essentially identical regardless of the subscriber's location and access port. For example, Fig. 6 also depicts generally an embodiment of the invention in which the permanent subscriber location 108 routinely interfaces with the ATM network 102 via an SVC connection established on a per connection basis.

[0060] At step s600, the subscriber accesses the ATM network 102 from a port other than the permanent access port with which the ATM network 102 ordinarily associates the subscriber. Accessing the ATM network 102 entails running the application software 124 at step s602, which initiates the process by sending a

conventional signaling protocol message requesting an SVC connection. In the system depicted in Fig. 6, the signaling protocol message is received by the exemplary ATM switch 103 at step s604.

[0061] The subscriber is then authorized at step s606 based on the subscriber's identification data embedded in the signaling protocol message, as described above with respect to steps s508 and s510 of Fig. 5. In particular, the protocol message may include, for example, a user identification number stored in the CallingPartyNumber field of an ATM SETUP message sent and an encrypted password stored in the CallingPartySubaddress field of the ATM SETUP message.

[0062] ATM switch 103 forwards the signaling protocol message to the registration server 112, which authenticates the subscriber based on stored information, as described above. If the identification data provided in the signaling protocol message does not match the subscriber's identification data in the registration server 112, the registration server 112 instructs the ATM switch 103 to reject the SVC connection request at step s620, terminating the SVC connection process.

[0063] If, however, the authentication is successful, the subscriber is presented the option of registering the remote access port 106 at step s608 of Fig. 6. For example, a message is sent to the nomadic user terminal 104 specifically asking whether the subscriber wishes to register the location. To perform step s608 in this manner, the registration server 112 sets up a temporary connection, e.g. an SVC connection, with the subscriber at the remote access port 106. The nomadic user terminal 104 receives the connection and the software application 124 responds by querying the subscriber whether port registration is desired. In an embodiment, the software application 124 runs a dialog box that enables the subscriber to check YES or NO next to the registration inquiry. The response is sent to the registration server 112, which terminates the SVC connection and proceeds accordingly.

[0064] In an alternative embodiment, the subscriber interaction with respect to registration occurs when the application software 124 is initially run at step s602. The application software 124 presents the registration query, in the form of a dialog box, for example, prior to sending the conventional signaling protocol message requesting the SVC connection. As described above, the subscriber selects YES to register the address of the remote access port 106 or NO to keep the registration information the same. The application software 124 then sends the subscriber's registration response in the conventional signaling protocol message, along with the initial SVC connection request, which the ATM switch 103 forwards to the registration server 112. In this embodiment, the registration server 112 determines at step s608 whether to register the address of the remote access port 106 by simply reading the previously obtained registration response.

[0065] In both embodiments, when the subscriber elects not to register the location (or when the subscriber does not have the ability to register the location), the registration data in the registration server 112 remains unchanged. All SVC connection requests will continue to be terminated at the subscriber's ATM address currently stored in registration server 112. The process then proceeds to step s614 to retrieve the subscriber's personalized service policies from the subscriber profile database 110. If at step s608 the registration server 112 determines that the subscriber has elected to register the remote access port 106, the registration server 112 sets the SVC terminating address to the address of the remote access port 106 at step s610. The ATM network 102 then correlates the subscriber's personal ATM address with the location address of the network port on which the connection has been established, i.e., remote access port 106. If the subscriber has a permanent subscriber location 108 that has already been associated with the subscriber's personal ATM address, the ATM address of remote access port 106 will be substituted for the ATM address of

the permanent subscriber location. All SVC connection requests addressed to the subscriber's personal ATM address will then be automatically terminated at the nomadic user terminal 104 through the remote access port 106. Alternatively, the subscriber may identify any ATM address at step s610, i.e., not necessarily the address of the remote access port 106, as the registered SVC connection terminating address, discussed below.

[0066] Regardless of whether the subscriber elects to register the access port address, the subscriber is associated with his or her personalized services. The personalized service policies are provided by the subscriber profile database 110 at step s614 to the registration server 112. These service policies are preestablished contractually between the subscriber (or the subscriber's group) and the ATM network provider. Based upon the retrieved service policies, the registration server 112 first determines at step s616 whether the subscriber is authorized to establish the requested SVC connection based on the retrieved service policies. Alternatively, the subscriber profile database 110 provides the service policy information directly to the ATM switch 103. If the subscriber is not authorized to establish the requested SVC connection, the ATM switch 103 rejects the SVC connection request at step s620, ending the process. If the service policies indicate that the subscriber is authorized to establish an SVC connection, the SVC connection is established through the remote access port 106 at step s618.

[0067] Significantly, as described above, the authentication step s606 may be performed transparently to the subscriber. Because the user identification number and password have been previously embedded in the protocol message, no interactive steps need be performed by the subscriber during the connection process. In other words, the subscriber is not queried to enter any numbers, passwords or ATM addresses in order to establish the requested connection with the network or to

implement the personalized service policies. As a result, the connection process from the remote access port 106 is quick and efficient. Also, the subscriber does not need to memorize numbers or passwords for simply connecting with the network. This is especially advantageous when the subscriber is required to input additional identification numbers and/or passwords to execute selected services within the ATM network 102 after establishing the SVC connection, or to execute selected services connectable through the ATM network 102, such as the Internet 120.

[0068] Because the authentication is performed on a per connection basis, multiple users can simultaneously use the same network connection. The ATM network 102 can accurately associate SVC connection requests to the respective originating subscribers and apply the correct corresponding service policies based on the independent identification of each subscriber. Also, a single individual may have more than one subscriber identity from the ATM network's point of view, e.g., a subscriber may pay for a publicly available version of a service, as well as belong to a corporate closed user group with access to the same service with different rights and privileges. In this situation, the individual subscriber has two different user identification numbers, yet is able to receive correct service for each user identification number on the same access port and simultaneously, if so desired.

[0069] In the embodiment of the invention depicted in Fig. 6, the same service options as described above are available upon dynamically registering the subscriber. For example, the subscriber may respond to the registration query at step s608 with a "forward-to" ATM address, to which the ATM network 102 will forward all connections addressed to the subscriber's personal ATM address. The "forward-to" address provided by the subscriber is different from both the remote access port 106 address and the permanent subscriber location 108 address. A "forward-to" address

may include, for example, a message center address or a personal assistant's address, which the subscriber would like to have handling incoming connections.

[0070] The registration process may also include additional flexibility to the subscriber, extending beyond simply registering access port addresses. For example, the application software 124 may enable various options for the subscriber to customize the extent of registration, such as specifying an alternative, e.g., forward-to," access port address only for attempted connections from preferred ATM addresses, pre-identified by the subscriber. The subscriber is then able to accept, for example, incoming connections from only his or her home office, assistant, family members, or other high priority sources. Such customized registration may better suit the subscriber's needs than simply registering a new address for all terminating connections.

[0071] Fig. 7 is a flowchart depicting the process of a subscriber accessing the ATM network 102 through the remote access port 106, but without automatic authentication for SVC privileges or automatic registration of the remote access port 106 used. The subscriber is therefore interactively provided options to qualify for SVC connections according to the subscriber's service policies, as well as to register the access port in the course of the connection process. Although Fig. 7 depicts a subscriber accessing the ATM network from a port other than his or her permanent subscriber location 108, the process is essentially identical regardless of the subscriber's location and access port.

[0072] At step s700, the subscriber accesses the ATM network 102 from a port other than the permanent access port with which the ATM network 102 ordinarily associates the subscriber. Accessing the ATM network 102 entails running the application software 124 at step s702, which initiates the process by sending a conventional signaling protocol message requesting an SVC connection. In the

system depicted in Fig. 7, the signaling protocol message is received by the exemplary ATM switch 103 at step s704.

[0073] Unlike the system depicted in Figs. 5 and 6, the signaling protocol message received by the ATM switch 103 and forwarded to the registration server 112, does not contain all of the data needed for full authentication of the subscriber. For example, the message may contain no authentication data, although the more likely scenario is that the message contains only the subscriber's identification number and no password. Therefore, at step s706, the subscriber is prompted to enter the missing authentication data, as determined by the registration sever 112. In order to prompt the subscriber, the registration server 112 must first establish an SVC connection with the remote access port 106, as described above with respect to interactive registration at step s608 of Fig. 6. Assuming the subscriber's identification number is embedded in the signaling protocol message, as described above, the subscriber enters the associated password. If the identification data provided by the subscriber and/or the signaling protocol message does not match the subscriber's identification data in the registration server 112, the registration server 112 instructs the ATM switch 103 to reject the SVC connection request at step s720, terminating the SVC connection process.

[0074] If, however, the authentication is successful, the registration server 112 determines whether the access port presently used by the subscriber, e.g., the remote access port 106, is currently registered. If it is, the process simply proceeds to step s714 and retrieves the personalized service policies associated with the subscriber. If the address of the remote access port 106 is not registered in the registration server 112, the subscriber is queried at step s710 whether registration of the access port address is desired. If not, the process proceeds to step s714 and retrieves the personalized service policies associated with the subscriber the subscriber. However,

because the subscriber has not registered, any SVC connection requests directed to the subscriber's personal ATM address will not be terminated to currently used access port. If the subscriber elects to register the address of the remote access port 106 at step s710, the registration server 112 sets the SVC terminating address to the address of the remote access port 106 at step s712. The ATM network 102 then correlates the subscriber's personal ATM address with the location address of the network port on which the connection has been established, i.e., remote access port 106.

[0075] Regardless of the various access port registration options, the subscriber is ultimately associated with his or her personalized services policies at step s714, which may be provided by the subscriber profile database 110 to the registration server 112. As previously discussed in regard to other embodiments of the invention, these service policies are preestablished contractually between the subscriber (or the subscriber's group) and the ATM network provider. Based upon the retrieved service policies, the registration server 112 first determines at step s716 whether the subscriber is authorized to establish SVC connections based on the retrieved service policies. Alternatively, the subscriber profile database 110 provides the service policy information directly to the ATM switch 103. If the subscriber is not authorized to establish an SVC connection, the ATM switch 103 rejects the SVC connection request at step s720, ending the process. If the service policies indicate that the subscriber is authorized to establish an SVC connection, the SVC connection is established through the remote access port 106 at step s718. The ATM network connection is then processed according to the subscriber's personalized service policies at step s722.

[0076] The invention has been described with reference to several exemplary embodiments, although it is understood that the words that have been used are words of description and illustration, rather than words of limitation. Changes may be made

within the purview of the appended claims, as presently stated and as amended, without departing from the scope and spirit of the invention in its aspects. Although the invention has been described with reference to particular means, materials and embodiments, the invention is not intended to be limited to the particulars disclosed; rather, the invention extends to all functionally equivalent structures, methods and uses such as are within the scope of the appended claims.

[0077] In accordance with various embodiments of the present invention, the methods described herein are intended for operation as software programs running on a computer processor. Dedicated hardware implementations including, but not limited to, application specific integrated circuits, programmable logic arrays and other hardware devices can likewise be constructed to implement the methods described herein. Furthermore, alternative software implementations including, but not limited to, distributed processing or component/object distributed processing, parallel processing, or virtual machine processing can also be constructed to implement the methods described herein.

[0078] It should also be noted that the software implementations of the present invention as described herein are optionally stored on a tangible storage medium, such as: a magnetic medium such as a disk or tape; a magneto-optical or optical medium such as a disk; or a solid state medium such as a memory card or other package that houses one or more read-only (non-volatile) memories, random access memories, or other re-writable (volatile) memories. A digital file attachment to email or other self-contained information archive or set of archives is considered a distribution medium equivalent to a tangible storage medium. Accordingly, the invention is considered to include a tangible storage medium or distribution medium, as listed herein and including art-recognized equivalents and successor media, in which the software implementations herein are stored.